World Transactions on Engineering and Technology Education
Vol.13, No.2, 2015

New approaches to experiment-based teaching in an information security course

Mengjia Yin, Tao Zhang, Xiaowen Chen & Conghuan Ye

Hubei Engineering University
Xiaogan, Hubei, People's Republic of China

ABSTRACT: Information security methods and techniques are evolving constantly, as new approaches emerge with the progress of technology, security threats and changes in society. Experiments are the main form of teaching an information security course. The course should integrate new knowledge with new technology. The approach presented in this article updates and extends the approach in an earlier article by Zhang et al [1]. The authors designed a multi-level experiment system; students can carry out experiments at different levels and orientations, as well as discussing and analysing the experimental process and data. This system helps students better understand, or even master, theoretical knowledge and improves their practical abilities. In the design of an experiment, attention should be paid to the authenticity of the experimental environment. Thus, information security experiments significantly facilitate and reinforce students' understanding of networking, security concepts and challenges. It also improved students' autonomous learning, and their practical, problem-solving abilities. Hence, students are better adapted to the needs of their future work.

INTRODUCTION

In recent years, information security has emerged as a computer discipline, which has garnered much academic research interest and received widespread public attention. Information security is an interdisciplinary subject. On the one hand, it has a profound, theoretical basis, which involves computers, mathematics, electronics, communications, and even management, ethics and many other disciplines. On the other hand, it has widespread application, including the military, finance, education and many industries. The industries include some in which people are deeply involved in their daily lives. In education, information security provides opportunities and challenges. Students need to study the theory and complex algorithms. But, the theory is not just a concept without application; and it is also important to strengthen the experiment-based teaching.

Pheils described a curriculum as being not a static tool for education, but rather, it should be continually assessed and adapted to achieve the best possible learning outcomes and experience for students through increasing satisfaction, understanding and motivation to learn [2]. Ben Othmane emphasised that security laboratories must train the students not just in *security hacking* but also in a broad range of security concepts and challenges [3]. Narayan provided a document with background material on possible experiments. In doing these experiments, students learn various steganography techniques (hiding messages inside other messages); Windows password hashing; Microsoft Baseline Security Analyser (a tool for determining the security status of a software system); and key ideas in encryption, etc [4]. Song presented on a cloud platform a digital forensics course, which broadens students' knowledge of cloud forensics technology [5]. Huang presented specific teaching plans for a virtualisation platform for an experiment-based teaching centre [6].

In this article, engineering education is considered. A variety of ways are outlined to improve students' practical abilities through experiment-based teaching. The aims of the experiment teaching are analysed, and the experiment contents designed. The design of the multi-level experiment system allows students to carry out experiments at different levels and content. Students can discuss and analyse the experimental process and data. This system helps them better understand, and even master, the theoretical knowledge and improves their practical abilities.

At the same time, the system provides the teachers engaged in network and information security research with a good platform for experiments. The approach presented in this article updates and extends the approach included in an earlier article by Zhang et al [1].

THE FUNCTION OF AN INFORMATION SECURITY LABORATORY

With experiments being the main practical teaching method for an information security course, attention needs to be paid to the authenticity of the experimental environment, to develop students' safety awareness. The difference between an information security experiment and other computer experiments is this: the information security experiment tends to use private network security devices and computers with installed special devices. Therefore, in the construction of a laboratory for teaching an information security course, the following considerations apply.

Scientific Research

In order to better support research work, active research areas in information security technology should be determined to feed into the design of the laboratory. Combined with support for the research needs of teachers and students, the laboratory should provide a good environment for supporting research. The laboratory can be used to carry out scientific research and practical work related to information security theory, as well as to security frameworks, security mechanisms and security technology. The laboratory should be proactive in accommodating future developments of the subject by being extensible and compatible with many other systems.

Practical Teaching

The primary function of the laboratory is practical teaching. Therefore, the laboratory equipment, including servers and routers, should primarily support the course experiments via an open experimental platform. At the same time, consideration should be given to some auxiliary requirements. For example, teachers need tools to produce courseware; systems are needed for performing demonstrations; and students need to be provided with teaching resources to download. Teachers also use the server platform to correct reports of experiments, to record attendance and grades, and to distribute documents, etc.

Information security experiments can involve damaging attacks on the experiment platform. However, the needs of daily teaching must be considered and this requires a stable network environment. This also requires a distinction between servers supporting the teaching and other equipment. Normal support schemes need to be in place, such as setting system hardware and software parameters, backup and fast recovery. A continuous, orderly practical teaching environment should be provided while, at the same time, also providing a more open environment by which students can experiment and learn through practice.

REQUIREMENTS FOR PRACTICAL TEACHING

The core requirement for developing innovative ability is the innovative experiment. These experiments develop the innovative abilities of students and are an important part of the information security curriculum. In practical teaching, students should continue to explore and summarise their findings and knowledge, to improve their practical ability and capacity for independent innovation. In turn, this stimulates students' enthusiasm for practical innovation and enhances their sense of satisfaction and self-confidence. The information security practical teaching has two main goals, which are discussed below.

Understanding the Basic Concepts, Principles and Mechanisms of Information Security

The information security course includes many abstract concepts; for example, access control, security models and complex algorithms, such as those for encryption and authentication. Because undergraduate students rarely encounter information security, they find the theoretical knowledge hard to understand. Therefore, it is the authors' hope that through the practical teaching of information security, students will better understand the basic concepts, principles and mechanisms of information security. In turn, this will allow students to understand actual implementations of information security theory.

Applying Information Security Knowledge

The practical teaching of information security should develop the students' ability to use information security knowledge in real applications. This is important in satisfying a student's future job demands. The people engaged in the computer industry require knowledge of information security, but information security requires more and different knowledge.

DESIGN OF AN EXPERIMENT

Reflecting the practical teaching requirements, the authors have designed various experiments. There are three types of experiment: basic verification, comprehensive, and design and innovation. The purpose of a basic verification experiment is to train students' basic operating abilities. Teachers provide students with the experimental plan and steps and the students, then, complete the experiment. Examples include cryptography foundation and operating system security experiments.

The purpose of comprehensive experiments is to cultivate students' ability to use their analytical skills to apply theoretical knowledge, so as to deepen the understanding of theoretical knowledge and its application for concrete applications. The purpose of the design and innovation experiments is to develop students' innovative and design abilities and to nurture team co-operation. In this type of experiment, the students are provided only with the experimental goals and requirements. The students must design and implement the experiment by themselves. Therefore, students must possess solid knowledge of information security theory and programming. The specific content of experiments and schedules are shown in Table 1.

Table 1: Experiment contents and schedule.

Sequence	Subject	Periods
1	Network information collection and vulnerability scanning	2
2	Network data acquisition and analysis	2
3	Network attack	4
4	Interception and cracking passwords	2
5	Data encryption, decryption and transmission	2
6	Firewalls	2
7	Intrusion detection	2
8	Integrated network attack and defence	8

As an indication of tasks required to complete the network information collection and vulnerability scanning experiment, students need to master the methods of information collection, use a common scanner to analyse the data, explain the relationship between the data and software loopholes, master network scanner programming and understand common scanner software, such as SATAN (security administrator tool for analysing networks), Time, CIS (contact image sensor) or Superscan, Digital X-ray Scan and the Nmap (network mapper).

This experiment first requires students to use the scanner software to scan the laboratory network host and, then, analyse the results. By evaluation of the network system security, rational decisions can be made to shut down dangerous ports. Nmap's vulnerability scanning includes many types of scan option so as to detect and display nodes. A scan range can be specified, and this avoids the need to type in a large number of IP addresses and host names. Students check their host's IP address, determine the scope of the scanning and, then, upload the scan results.

The experiment, network data acquisition and analysis require students to master the methods of acquisition and analysis of network data. They need to understand the use of sniffer (a tool for capturing network data), how to analyse sniffer data, and explain the relationship between the data and network security; hence, solving the problems of the monitored system and strengthening its network security system. Students need to master Wireshark, which is an open-source, free download system for analysing communication packets. It is usually used in network troubleshooting, monitoring abnormal packets, software packet error detection, and so on. Wireshark supports a variety of operating systems: Windows and variants of UNIX and MAC. With this software, students can grab data packets and analyse detailed information in the packets. Students use Wireshark software to visit all packets at an FTP (file transfer protocol) site and, then, upload the results.

The experiment, network attack, requires that students master the methods and principle of the network attack. They exploit system vulnerabilities to implement denial of service, spoofing, back door and Trojan attacks. Students must master the programming requirements of the various attacks. So as to further grasp the common attack methods and preventive measures, methods to prevent and remove Trojan malware are covered. The methods and tools used in this experiment can cause great damage. Therefore, students are required to operate in a virtual machine environment to avoid damage to computers in the real network.

The experiment, interception and cracking of passwords require that students master the methods of password cracking and interception. The students are required to remotely crack a Windows Server 2000 user password using VMware to obtain the username and password.

The experiment, data encryption, decryption and transmission include classic DES (data encryption standard) and RSA (Rivest Shamir Adleman) cryptography algorithms. In this experiment, students use the DES algorithm to recover plain text from cipher text.

An Internet firewall enhances an organisation's internal network security by strengthening the network access control to prevent external users illegally using the Intranet resources, so as to damage network equipment or steal sensitive data. The experiment, firewalls, requires students to research network firewalls, including intrusion detection, security log analysis, security configuration and the system log. Students establish a Cisco PIX (private Internet exchange) firewall, study the PIX firewall security system and complete the security configuration. PIX is Cisco's hardware firewall and the hardware firewall works fast, while being convenient to use. PIX has many types and the number of simultaneous connections is an important parameter of the PIX firewall. Typical equipment is the PIX525, 635, 721, and so on.

In this experiment, students are required to configure IP parameters on the PIX interface, with configuration access control ICMP (Internet control message protocol), and the ping command is allowed to be used between three regions. Students configure the NAT (network address translation or network address translator, which is the virtualisation of

Internet protocol (IP) addresses), and the DMZ (demilitarised zone, sometimes referred to as a perimeter network, is a physical or logical subnetwork); the external IP is specified on its own. After the completion of the operation, the PIX configuration document is submitted to the FTP site.

The experiment, intrusion detection, complements the firewall experiment. This experiment requires students to monitor ports by which to collect key information and, by analysing the system log, determine whether there has been an attack on the system. Students learn to use an IDS (intrusion detection system), so as to dynamically manage a computer security system and resolve network security questions. Students investigate the main functions of IDS and data monitoring technology. The experiment uses a simulated Cisco router.

The integrated network attacks and defence experiment system is the core experiment of the information security curriculum. This experiment helps students grasp the content of network security technology and the basic knowledge of network security. This integrated experiment covers these subjects: scanning, network sniffing, password cracker, spoofing attacks, DOS (denial of services), buffer overflows, Web attacks, SQL (structured query language) injection, Trojan-horses, computer viruses, mobile phone viruses, firewalls and intrusion detection [7].

The practical teaching emphasises an organic combination of teaching, studying and practice. Students are divided into groups of six to eight, half of whom belong to the attackers and half to the defenders. This experiment develops students' practical, self-directed learning, problem analysis and problem-solving abilities. In addition, it develops a student's team organisation and collaboration abilities.

EFFECTIVE USE OF TEACHING METHODS

Educating a mix of information security students from different generations means teachers and students need to interact in a common space [8]. This requires an understanding of the characteristics and learning styles of each generation, plus the flexibility to adjust methods, so as to achieve learning objectives for the benefit of all.

In practical teaching, teachers should pay attention to the cultivation of an applicable, practical ability. Teachers traditionally use the task-driven teaching model, through which a specific task is introduced. The task is then analysed, solved, extrapolations identified and the task summarised. This blends learning and skills acquisition [9].

Teachers changed the traditional teaching mode of *the teacher as the centre, teaching material as the centre, cramming for examinations* to the mode of *student at the centre, ability as the goal, the students' active participation, autonomy, co-operation, exploration and innovation*. Teachers must now pay attention to cultivating students' practical ability and the application of knowledge.

Students should find information security problems in the process of using computers and networks. Identified problems and solutions improve students' active learning. Flexible teaching methods improve the students' interest in learning and let them actively take part in the experiments [10].

CONCLUSIONS

As a new discipline, the experiment-based teaching of information security has many problems, which need to be further explored. The course needs a synthesisation of the latest research in computer science and technology, and application of the information to the information security course experiments. The new theories and technologies need to be transmitted to young students in an appropriate way, so as to arouse their enthusiasm for autonomous learning. Students need to understand the basic theory and technology of the experiments, which will improve their ability to solve practical problems and, hence, adapt them to the needs of their future work.

ACKNOWLEDGEMENTS

This work is supported by the Hubei Engineering University Teaching Reform Project (No.2014B07). This work is also supported by the research project of Hubei Engineering University No. z2011007 and the Natural Science Foundation of Hubei Province of China under Grant No. 2015CFB236.

REFERENCES

1. Zhang, T., Yin, M. and Yang, Y., An experiment teaching mode for an *Introduction to Information Security* course. *World Trans. on Engng. and Technol. Educ.*, 12, **4**, 725-728 (2014).
2. Pheils, D., Applying a community project approach to IT and security courses. *Proc. 2013 Infor. Security Curriculum Develop. Conf.*, Kennesaw, GA, USA, 79-87 (2013).
3. Ben Othmane, L., Bhuse, V. and Lilien, L.T., Incorporating lab experience into computer security courses. *Proc. 2013 World Congr. on Computer and Infor. Technol.*, Sousse, Tunisia, 1-4 (2013).
4. Narayan, M., Teaching computer security with a hands-on component. *8th IFIP WG 11.8 World Conf. on Infor. Security Educ.*, Auckland, New Zealand, 204-210 (2013).

5. Song, X., Deng, H., Chen, L. and Wang, Z., Experimental teaching of a digital forensics course based on a cloud computing platform*.* *World Trans. on Engng. and Technol. Educ.*, 11, **3**, 237-242 (2013).
6. Huang, H., Chen, S. and Huang, C., Computer teaching based on experiments using a virtualisation platform. *World Trans. on Engng. and Technol. Educ.*, 11, **4**, 527-531 (2013).
7. Wei, W. and Li, P., Innovative teaching and learning experiences in network attacks and defense. *Proc. 2012 8th Inter. Conf. on Computational Intelligence and Security*, Guangzhou, China, 587-590 (2012).
8. Armstrong, H., Dodge R. and Armstrong C., Reaching today's information security students. *Proc. 8th IFIP WG 11.8 World Conf. on Infor. Security Educ.*, 218-225 (2013).
9. Zhang, T. and Yin, M., Applying humanistic values to computer practical teaching for quality education. *World Trans. on Engng. and Technol. Educ.*, 12, **2**, 298-301 (2014).
10. Fan, L., Methods for improving the professional level of students majoring in information and computer science. *World Trans. on Engng. and Technol. Educ.*, 12, **1**, 122-126 (2014).